REMARKS

The Examiner has rejected Claims 1-3, 5-9, 11-14, 16-22 and 24-30 under 35 U.S.C. 102(b) as being anticipated by Key Management for Large Dynamic Groups: One-Way Function Trees and Amortized Initialization, from the IRTF SMUG Meeting on March 15, 1999. Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 24 and 25, the Examiner has relied on Key Management's disclosure of re-keying using one-way function trees on page 5 to make a prior art showing of applicant's claimed technique "wherein upon eviction of at least one member of said group, said leaf key enables said members of said subgroup to receive an update message for an interior node above said leaf node" (see the same or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that generally teaching re-keying, as in Key Management, does not rise to the level of specificity of applicant's claim language. In particular, Key Management does *not* teach a "leaf key [that] enables said members of said subgroup to receive an update message for an interior node above said leaf node," as claimed by applicant (emphasis added). In fact, Key Management only teaches that a "group base key [is] derived from [a] system based key," where such system base key is "known only to [a] system manager" (see page 11). Thus, there is no "interior node above said leaf node" that is utilized in the manner claimed by applicant.

With respect to independent Claim 11, the Examiner has completely failed to address applicant's claimed "notifying a plurality of members of said group that said at least one member has been evicted." Simply nowhere in Key Management is there even a suggestion of notifying members that a member has been evicted. Instead, Key Management only very generally teaches that a group operation may include evicting a member from a session (see page 4).

With respect to independent Claim 17, the Examiner has again relied on Key Management's disclosure of re-keying using one-way function trees on page 5 to make a prior art showing of applicant's claimed "distributing key update messages for said hierarchical tree upon eviction of one or more members of said subgroup, wherein said distributed key update messages do not update keys associated with nodes below said common node."

Applicant respectfully asserts that the Examiner's reliance on only a general teaching of re-keying is insufficient to meet applicant's specific claim language. In particular, applicant claims that "said distributed key update messages do not update keys associated with nodes below said common node" (emphasis added). Applicant notes that nowhere in the Key Management reference is there any disclosure of such specific claim language, and especially not in the context claimed by applicant.

Still yet, with respect to each of the independent claims, the Examiner has relied on Key Management's disclosure of a group base key that is derived from a system base key (page 11) to make a prior art showing of applicant's claimed technique "wherein each of said members of said subgroup is capable of independently updating a shared interior node key" (see the same or similar, but not identical language in each of the independent claims).

Applicant respectfully asserts that Key Management teaches a "[g]roup base key [that is] derived from [a] system base key," where the system base key is established using a "[p]airwise authenticated key exchange" (see page 11-emphasis added). In fact, applicant notes that the pairwise key in Key Management is "known only to [the] system manager." Thus, since the group key is derived from the pairwise key known only by the system manager, Key Management actually *teaches away* from applicant's specific claim language. In particular, in Key Management, each individual member of a subgroup would *not* be "capable of independently updating a shared interior node key," as claimed by applicant since only the system manager would know the pairwise key from which the shared interior key would be derived.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.* 868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the Key Management reference, as noted above. A notice of allowance or a specific prior art showing of each of the foregoing claimed features, in combination with the remaining claimed features, is respectfully requested.

The Examiner has further rejected Claims 1, 3, 6-9, 11-14, 17, 19-22 and 24-30 under 35 U.S.C. 103(a) as being unpatentable over "Ioulus: A Framework for Scalable Secure Multicasting" by Mittra, in view of Li (U.S. Patent No. 6,606,706) in further view of "Dynamic Cryptographic Context Management (DCCM), Report #4" by Balenson. Applicant respectfully disagrees with such rejection.

With respect to independent Claims 1, 24 and 25, the Examiner has relied on Col. 10, lines 5-14 and Col. 11, lines 13-43 in Li to make a prior art showing of applicant's claimed "leaf key [that] enables said members of said subgroup to receive an update message for an interior node above said leaf node." Applicant respectfully asserts that such excerpts only teach a "primary top regional security broker [that] receives the announcement and distributes it globally." However, nowhere in Li is there even a suggestion of a "leaf key [that] enables said members of said subgroup to receive an update message," as claimed by applicant (emphasis added). In addition, in Li the top regional security broker distributes the announcement globally and "[e]ach security broker...forwards it downstream," whereas applicant claims that the members "receive an update message for an interior node above said leaf node" (emphasis added).

With respect to independent Claim 11, the Examiner has completely failed to address applicant's claimed "notifying a plurality of members of said group that said at least one member has been evicted." Applicant respectfully asserts that simply nowhere in the prior art is there even a suggestion of notifying members that a member has been evicted.

With respect to independent Claim 17, the Examiner has also failed to address applicant's claimed "distributing key update messages for said hierarchical tree upon eviction of one or more members of said subgroup, wherein said distributed key update messages do not update keys associated with nodes below said common node." Applicant notes that Li even *teaches away* from applicant's claim language since Li teaches a "primary top regional security broker [that] receives the announcement and distributes it globally" and that "[e]ach security broker...forwards it downstream" (emphasis added-see Col. 10, lines 5-14).

Still yet, with respect to each of the independent claims, the Examiner has relied on Baleson's disclosure in 5.2.2 OFT operations on page 7 to make a prior art showing of applicant's claimed technique "wherein each of said members of said subgroup is capable of independently updating a shared interior node key" (see the same or similar, but not identical language in each of the independent claims).

Specifically, the Examiner has relied on Baleson's teaching that "each member establishes an individual group base key known only by the member and the group manager." However, applicant notes that such individual group base key is only established during group induction, and not when a member is evicted. In fact, Balenson teaches that after a member has been evicted, new keys are broadcasted to subgroups so that members can construct a new group key, and not that the members independently update a shared interior node key. Furthermore, during induction, "each member establishes an individual group base key known only by the member and the group manager" (emphasis added). Clearly, a key known only by the member and the group manager does not meet applicant's claimed "subgroup [that] is capable of independently updating a shared interior node key" as claimed by applicant (emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 5 and 28 et al. into each of the independent claims. In addition, applicant has incorporated the subject matter of Claim 29 into independent Claims 1 and 11 and the subject matter of Claim 30 in to independent Claims 17, 24 and 25.

With respect to the subject matter of Claims 5 and 28-30 et al., as rejected under 35 U.S.C. 102(b) as being anticipated by Key Management, it is noted that the Examiner has not even specifically addressed the specific claim limitations of the instant claims. Further, after careful review of the entire Key Management reference, it is noted that there is not even a suggestion of a self-repairing group that uses a reusable power set, where the reusable power set uses a power set of said members in said subgroup as a basis for updates, and the reusable power set includes 2^N or $2^N - 1$ sets, where N includes the number of said members, as claimed.

With respect to the subject matter of Claim 5 et al., as rejected under 35 U.S.C. 103(a) as being unpatentable over Mittra, Li. Balenson and Dondeti (U.S.

Patent No. 6,240,188), the Examiner has relied on Col. 3, line 47-Col. 4, line 65 from Dondeti to make a prior art showing of applicant's claimed technique "wherein said self-repairing ... group uses a reusable power set." However applicant notes that nowhere in such excerpt is there any disclosure of a "reusable power set," let alone in the context claimed by applicant. Specifically, such excerpt from Dondeti only teaches that a "join/leave requires only keys in the path to the root from the joining/departing host to be changed," but not that any sort of power set is utilized.

With respect to the subject matter of Claim 28, as further rejected under 35 U.S.C. 103(a), the Examiner has relied on sections 5.2.2 to 5.2.3. on pages 7-8 of Balenson to make a prior art showing of applicant's claimed technique "wherein said reusable power set uses a power set of said members in said subgroup as a basis for ... updates." Applicant notes that section 5.2.2. only generally discloses that "blinded node keys that have changed are broadcast securely to the appropriate subgroups, allowing all members to construct the new group key." However, nowhere in such section of Balenson is there any suggestion of how such new group key is constructed, let alone where a "reusable power set uses a power set of said members in said subgroup as a basis for ... updates," as claimed by applicant.

In addition, section 5.2.3 from Balenson, as relied on by the Examiner, only relates to the number of keys stored by group members and the computations efforts required for re-keying among an entire group. Specifically, such excerpt teaches that "the number of keys stored by group members, then number of keys broadcast to the group when new members are added or evicted, and the computational efforts of group members, are logarithmic in the number of group members." Clearly, such teaching is not even associated with "a basis for ... updates," as claimed by applicant. Furthermore, nowhere in section 5.2.3 or the entire Balenson reference is there any disclosure of a "reusable power set [that] uses a power set of said members in said subgroup as a basis for ... updates" as specifically claimed by applicant (emphasis added).

With respect to the subject matter of Claims 29 and 30, as further rejected under 35 U.S.C. 103(a), the Examiner has again relied on section 5.2.2 on pages 7-8

of Balenson to make a prior art showing of applicant's claimed techniques "wherein said reusable power set includes 2^N sets, where N includes the number of said members" (Claim 29) and "wherein said reusable power set includes $2^N - 1$ sets, where N includes the number of said members" (Claim 30). Specifically, the Examiner argues that adding a member would be based on 2^N and that evicting a member would be based on 2^{N-1}. Applicant respectfully asserts that, for the reasons given with respect to Claim 28 above, such excerpt does not teach any sort of reusable power set in the context claimed by applicant. Again, Balenson does *not* teach that any sort of set is utilized, as claimed by applicant, but instead only generally discloses that "blinded node keys that have changed are broadcast securely to the appropriate subgroups, allowing all members to construct the new group key."

Again, applicant respectfully asserts that at least the third element of the prima facie case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or a proper prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

To this end, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. If any fees are due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P090/00.176.01).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172
Telephone: (408) 505-5100